United States Government Accountability Office

GAO

Report to Congressional Requesters

May 2007

# DEFENSE INFRASTRUCTURE

# Actions Needed to Guide DOD's Efforts to Identify, Prioritize, and Assess Its Critical Infrastructure


GAO-07-461

# Report Documentation Page

*Form Approved*
*OMB No. 0704-0188*



| 1. REPORT DATE | 2. REPORT TYPE | 3. DATES COVERED |
|---|---|---|
| **MAY 2007** | | **00-00-2007 to 00-00-2007** |

| 4. TITLE AND SUBTITLE | 5a. CONTRACT NUMBER |
|---|---|
| **Defense Infrastructure. Actions Needed to Guide DOD's Efforts to Identify, Prioritize, and Assess Its Critical Infrastructure** | 5b. GRANT NUMBER |
| | 5c. PROGRAM ELEMENT NUMBER |
| 6. AUTHOR(S) | 5d. PROJECT NUMBER |
| | 5e. TASK NUMBER |
| | 5f. WORK UNIT NUMBER |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Government Accountability Office,441 G Street NW,Washington,DC,20548** | 8. PERFORMING ORGANIZATION REPORT NUMBER |
| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES) | 10. SPONSOR/MONITOR'S ACRONYM(S) |
| | 11. SPONSOR/MONITOR'S REPORT NUMBER(S) |

12. DISTRIBUTION/AVAILABILITY STATEMENT
**Approved for public release; distribution unlimited**

13. SUPPLEMENTARY NOTES
**The original document contains color images.**

14. ABSTRACT

15. SUBJECT TERMS

| 16. SECURITY CLASSIFICATION OF: | | | 17. LIMITATION OF ABSTRACT | 18. NUMBER OF PAGES | 19a. NAME OF RESPONSIBLE PERSON |
|---|---|---|---|---|---|
| a. REPORT | b. ABSTRACT | c. THIS PAGE | | | |
| **unclassified** | **unclassified** | **unclassified** | | **48** | |

May 2007

# DEFENSE INFRASTRUCTURE

# Actions Needed to Guide DOD's Efforts to Identify, Prioritize, and Assess Its Critical Infrastructure

GAO Accountability·Integrity·Reliability

Highlights

Highlights of GAO-07-461, a report to congressional requesters

## Why GAO Did This Study

The Department of Defense (DOD) relies on a network of DOD and non-DOD infrastructure assets in the United States and abroad so critical that its unavailability could hinder DOD's ability to project, support, and sustain its forces and operations worldwide. DOD established the Defense Critical Infrastructure Program (DCIP) to identify and assure the availability of mission-critical infrastructure. GAO was asked to evaluate the extent to which DOD has (1) developed a comprehensive management plan to implement DCIP and (2) identified, prioritized, and assessed its critical infrastructure. GAO analyzed relevant DCIP documents and guidance and met with officials from more than 30 DOD organizations that have DCIP responsibilities, and with Department of Homeland Security (DHS) officials involved in protecting critical infrastructure.

## What GAO Recommends

GAO recommends DOD take several actions to improve the efficiency and effectiveness of DCIP operations. Actions include developing a comprehensive management plan; issuing a chartering directive defining the relationship between the directorates responsible for DCIP and antiterrorism missions; and identifying non-DOD-owned critical infrastructure for DHS to consider in its assessments. DOD concurred with all of GAO's recommendations.

www.gao.gov/cgi-bin/getrpt?GAO-07-461.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Davi M. D'Agostino at (202) 512-5431 or dagostinod@gao.gov.

## What GAO Found

While DOD has taken important steps to implement DCIP, it has not developed a comprehensive management plan to guide its efforts. GAO's prior work has shown the importance of developing a plan that incorporates sound management practices, such as issuing guidance, coordinating stakeholders' efforts, and identifying resource requirements and sources. Most of DOD's DCIP guidance and policies are either newly issued or in draft form, leading some DOD components to rely on other, better-defined programs, such as the antiterrorism program, to implement DCIP. Although DOD issued a DCIP directive in August 2005, the lead office responsible for DCIP lacks a chartering directive that defines important roles, responsibilities, and relationships with other DOD organizations and missions. DOD has created several information sharing and coordination mechanisms; however, additional measures could be taken. Also, DOD's reliance on supplemental appropriations to fund DCIP makes it difficult to effectively plan future resource needs. Until DOD completes a comprehensive DCIP management plan, its ability to implement DCIP will be challenged.

DOD estimates that it has identified about 25 percent of the critical infrastructure it owns, and expects to identify the remaining 75 percent by the end of fiscal year 2009. In contrast, DOD has identified significantly less of the critical infrastructure that it does not own, and does not have a target date for its completion. Among the non-DOD-owned critical infrastructure that has been identified are some 200 assets belonging to private sector companies that comprise the defense industrial base—the focus of another report we plan to issue later this year. DOD estimates that about 85 percent of its mission-critical infrastructure assets are owned by non-DOD entities, such as the private sector; state, local, and tribal governments; and foreign governments. DOD has conducted vulnerability assessments on some DOD-owned infrastructure. While these assessments can provide useful information about specific assets, until DOD identifies and prioritizes all of the critical infrastructure it owns, assessment results have limited value for deciding where to target funding investments. For the most part, DOD cannot assess assets it does not own, and DOD has not coordinated with DHS to include them among DHS's assessments of the nation's critical infrastructure. DOD has delayed coordinating the assessment of non-DOD-owned infrastructure located abroad while it focuses on identifying the critical infrastructure that it does own. Regarding current and future DCIP funding levels, they do not include the cost to remediate vulnerabilities that are identified through the assessments. When DOD identifies, prioritizes, and assesses its critical infrastructure, and includes remediation in its funding requirements, its ability to perform risk-based decision making and target funding to priority needs will be improved.

# Contents

**Abbreviations**

| | |
|---|---|
| ASD(HD&ASA) | Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs |
| COCOM | Combatant Command |
| DCIP | Defense Critical Infrastructure Program |
| DHS | Department of Homeland Security |
| DOD | Department of Defense |
| DTRA | Defense Threat Reduction Agency |
| PCII | Protected Critical Infrastructure Information |

GAO
Accountability * Integrity * Reliability

**United States Government Accountability Office**
**Washington, DC 20548**

May 24, 2007

The Honorable Solomon P. Ortiz
Chairman
The Honorable Jo Ann Davis
Ranking Member
Subcommittee on Readiness
Committee on Armed Services
House of Representatives

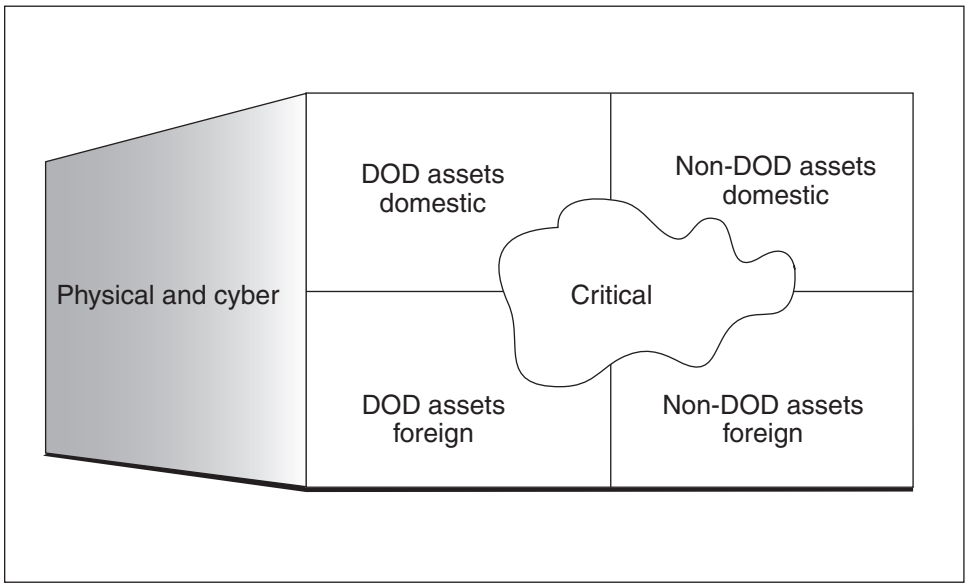
The Honorable W. Todd Akin
House of Representatives

The Department of Defense (DOD) relies on a network of physical and cyber infrastructure so critical that its incapacitation, exploitation, or destruction could have a debilitating effect on DOD's ability to project, support, and sustain its forces and operations worldwide. This defense critical infrastructure consists of DOD and non-DOD assets located within and outside the United States (see fig. 1). According to DOD, about 85 percent of the infrastructure it relies on is owned by non-DOD entities.[1] Because of its importance to DOD operations, defense infrastructure represents an attractive target to adversaries; but it is also vulnerable to natural disasters and accidents. DOD has recognized and emphasized the importance of ensuring the availability of critical infrastructure in the most

[1]We did not independently verify the accuracy of this estimate. However, the estimate that non-DOD entities (i.e., private industry; state, local, and tribal governments; and foreign governments) own and operate approximately 85 percent of the nation's critical infrastructure is consistent with national-level estimates and is cited in several national strategies. See, for example, The White House, *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* (Washington, D.C.: February 2003) and Office of Homeland Security, *National Strategy for Homeland Security* (Washington, D.C.: July 2002).

recent versions of the *National Military Strategy*[2] and the *Quadrennial Defense Review Report*.[3]

**Figure 1: Notional Depiction of Infrastructure Available to DOD**




Source: GAO analysis of DOD information.

*Homeland Security Presidential Directive 7*,[4] issued in December 2003, designates the Secretary of the Department of Homeland Security (DHS) as the principal federal official responsible for leading, integrating, and coordinating the overall national effort to protect the nation's critical infrastructure and key resources. The Homeland Security Act of 2002[5] and

[2]Department of Defense, Joint Chiefs of Staff, *The National Military Strategy of the United States of America: A Strategy for Today; A Vision for Tomorrow* (Washington, D.C.: 2004). The *National Military Strategy* is the Joint Chiefs of Staff's document on the strategic direction of the armed forces, which establishes three military objectives: (1) protect the United States against external attacks and aggression, (2) prevent conflict and surprise attack, and (3) prevail against adversaries.

[3]Department of Defense, *Quadrennial Defense Review Report* (Washington, D.C.: Feb. 6, 2006). The Quadrennial Defense Review is a comprehensive internal review of DOD's forces, resources, and programs.

[4]*Homeland Security Presidential Directive 7* (Washington D.C.: Dec. 17, 2003).

[5]Pub. L. No. 107-296, Nov. 25, 2002.

the Presidential Directive also direct DHS to produce a national plan for critical infrastructure and key resources protection, and on June 30, 2006, DHS issued the *National Infrastructure Protection Plan*. This plan provides an overarching approach for protecting critical infrastructure and key resources against terrorist attacks, major disasters, and other emergencies. The cornerstone of the *National Infrastructure Protection Plan* is its risk-management framework to establish priorities based on risk, and determine protection and business continuity initiatives that provide the greatest mitigation of risk. The *National Infrastructure Protection Plan* identifies 17 infrastructure and key resources sectors, and designates one or more lead federal agencies—referred to as a sector-specific agency—for each sector. For example, the Departments of Defense and Energy are the sector-specific agencies for the Defense Industrial Base and the Energy sectors, respectively. DHS is the sector-specific agency for 10 of the 17 sectors. Sector-specific agencies are responsible for, among other things, coordinating with all relevant federal, state, and local governments and the private sector; encouraging risk management strategies; and conducting or facilitating vulnerability assessments of their sector.

*Homeland Security Presidential Directive 7* also requires all federal departments and agencies to identify, prioritize, and coordinate the protection of critical infrastructure and key resources from terrorist attacks. The Office of the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs (ASD[HD&ASA]), within the Office of the Under Secretary of Defense for Policy, serves as the principal civilian advisor to the Secretary of Defense on the identification, prioritization, and protection of DOD's critical infrastructure.[6] DOD established the Defense Critical Infrastructure Program (DCIP) to identify and assure the availability of mission-critical infrastructure. DCIP encompasses the full spectrum of threats—ranging from terrorist attacks to natural disasters and catastrophic accidents—that can adversely affect critical infrastructure. Earlier programs analogous to DCIP can be traced back to 1998. ASD(HD&ASA) has been responsible for developing and ensuring implementation of critical infrastructure protection policy and program guidance activities since September 2003. Within DOD, several

[6]The Office of the Under Secretary of Defense for Policy was reorganized in December 2006. This reorganization included, among other things, the Office of the Assistant Secretary of Defense for Homeland Defense being renamed the Office of the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs. Hereafter, this office is referred to by its current name.

organizations play a role in DCIP, including the combatant commands (COCOM) and the military services. DOD also identified 10 virtual, functionally-based defense sectors to consider critical infrastructure that cross traditional organizational boundaries. The 10 defense sectors are financial services; global information grid; intelligence, surveillance, and reconnaissance; space; health affairs; logistics; personnel; public works; transportation; and the defense industrial base. Over the last 4 fiscal years (2004 to 2007), DOD has spent about $160 million on DCIP.

In our recent report on DOD's collective protection for military forces,[7] we discussed DOD's collective protection management problems, including fragmented policies and operating concepts among the varied programs and organizations involved. DOD has been unable to reach consensus on what criteria to use to identify its most critical facilities. As we reported, these management problems make it difficult for DOD to balance competing needs and prudently allocate funding resources for collective protection improvements. We recommended, among other things, that DOD provide clearer, more consistent policies to guide the funding of collective protection and other installation preparedness activities.

As you requested, we have begun a body of work reviewing actions DOD has taken to identify, protect, and otherwise assure the availability of infrastructure necessary to sustain its operations. This initial report focuses on key organizational, structural, and programmatic aspects of DCIP. Specifically, this report evaluates the extent to which DOD has (1) developed a comprehensive management plan to implement DCIP and (2) identified, prioritized, and assessed its critical infrastructure. We plan to issue additional products of interest to you, including a report later this year that examines the defense industrial base. Accordingly, this report does not address the Defense Industrial Base defense sector, unless indicated otherwise.

To evaluate the extent to which DOD has developed a comprehensive management plan to implement DCIP, we reviewed and analyzed relevant DCIP guidance, met with key officials responsible for DCIP from the military services, the COCOMs (hereafter referred to in this report as "DOD components"), and the defense sector lead agents; several offices

[7]See GAO, *Chemical and Biological Defense: Updated Intelligence, Clear Guidance, and Consistent Priorities Needed to Guide Investments in Collective Protection*, GAO-07-113 (Washington, D.C.: Jan. 19, 2007).

within the Office of the Secretary of Defense; and the Joint Staff's Directorate for Antiterrorism and Homeland Defense. In addition, we reviewed and analyzed pertinent funding data from the past 4 fiscal years, met with the Office of the Under Secretary of Defense (Comptroller)/Chief Financial Officer to discuss the budgeting process, and interviewed officials responsible for determining funding requirements for the program. To evaluate the extent to which DOD has identified, prioritized, and assessed its critical infrastructure, we reviewed and analyzed relevant DCIP guidance including the *DCIP Assessment Standards and Benchmarks*[8] and *DCIP Criticality Process Guidance Document*.[9] We interviewed DOD officials responsible for critical infrastructure and reviewed DOD's critical infrastructure vulnerability assessment process. We also met with Defense Threat Reduction Agency (DTRA) officials involved in implementing infrastructure vulnerability assessments.

We conducted our work between June 2006 and May 2007 in accordance with generally accepted government auditing standards. A more thorough description of our scope and methodology is provided in appendix I.

## Results in Brief

While DOD has taken some important steps to implement DCIP, it has not developed a comprehensive management plan to guide its efforts. Our prior work,[10] as well as the *Standards for Internal Control in the Federal Government*,[11] emphasizes the importance of such a plan and management controls, respectively, to guide program implementation. Accordingly, this plan should include key elements, such as developing and issuing guidance, coordinating stakeholders' efforts, and identifying resource requirements and sources. DOD's most recent effort to protect critical infrastructure began in September 2003 and, as of May 2007, most of DOD's DCIP guidance was either newly issued or still in draft form. In the absence of finalized guidance, DOD components have been pursuing

[8]This guidance allows DOD components to determine vulnerabilities of their critical infrastructure.

[9]This guidance provides a framework for identifying and prioritizing defense critical infrastructure.

[10]See, for example, GAO, *Military Readiness: Navy's Fleet Response Plan Would Benefit from a Comprehensive Management Approach and Rigorous Testing*, GAO-06-84 (Washington, D.C.: Nov. 22, 2005).

[11]GAO, *Standards for Internal Control in the Federal Government*, GAO/AIMD-00-21.3.1 (Washington, D.C.: November 1999).

varying approaches to DCIP. For example, some components have relied on established programs, such as the antiterrorism program, to implement DCIP, even though antiterrorism has not been formally linked to DCIP. Although DOD issued a DCIP directive in August 2005, the lead office—ASD(HD&ASA)—lacks a chartering directive that defines important roles, responsibilities, and relationships with other DOD organizations and missions. In March 2003, the Deputy Secretary of Defense required the Director of Administration and Management within the Office of the Secretary of Defense to, among other things, define the relationship between the Directorates for HD&ASA and Special Operations and Low-Intensity Conflict and Interdependent Capabilities regarding several matters, including antiterrorism missions, in a chartering directive. However, as of May 2007, more than 4 years later, this task has not been accomplished. Similarly, because DOD's strategy on tracking and monitoring critical infrastructure was not issued until 2006, components have been collecting different information on their infrastructure, which, over the long term, could complicate information sharing and analysis across the DOD components and sector lead agents. To facilitate communication among stakeholders, DOD has established several information sharing and coordination mechanisms to promote a common approach to common issues, such as sponsoring the Homeland Infrastructure Foundation Level Database Working Group. The Working Group is a coalition of federal, state, and local government organizations, and private companies that are involved in collecting and mapping geographic information related to homeland defense. Existing DCIP guidance emphasizes information sharing and collaboration with relevant government and private-sector entities. However, we found that three of the five defense sector lead agents that have a federal-level counterpart do not routinely share information with their corresponding federal-level critical infrastructure sector counterparts due to the immaturity of the program.[12] DCIP has received about $160 million in funding from fiscal years 2004 to 2007.[13] However, the DOD components and sector lead agents have received only $68.5 million during the same 4-year period, of which $14.3 million (about 21 percent of the component and sector lead

[12]The Intelligence, Surveillance, and Reconnaissance; Logistics; Personnel; and Space defense sectors do not have a federal-level counterpart.

[13]The $160 million total does not include the $6.8 million provided to the Defense Contract Management Agency, the lead agent for the Defense Industrial Base defense sector during fiscal years 2004 to 2007. Further, the Marine Corps and the U.S. Pacific Command were unable to provide funding data for fiscal year 2004 because these data were unavailable.

agents' combined funding) has come from supplemental appropriations. Our prior work has shown that relying on supplemental appropriations is not an effective means for decision makers to plan for future years resource needs, weigh priorities, and assess budget trade-offs. Until DOD completes a comprehensive management plan to implement DCIP, which includes issuing remaining guidance and fully identifying funding requirements, its ability to implement DCIP will be challenged. We are making recommendations that DOD develop and implement a comprehensive management plan to guide DCIP implementation. This plan would establish timelines for finalizing and issuing DCIP guidance; assist the defense sector lead agents in identifying and including DCIP funding through the regular budgeting process; and determine funding levels and sources to avoid reliance on supplemental appropriations. We also are recommending that DOD issue a chartering directive that would, among other things, clarify the relationship between the department's DCIP and antiterrorism missions.

DOD estimates that it has identified about 25 percent of the critical infrastructure it owns, and DOD officials expect to finish identifying the remaining infrastructure assets that it controls (estimated to be about 15 percent of the total) by the fiscal year 2008–2009 time frame. The remainder of its mission-critical infrastructure (estimated to be about 85 percent of the total) is owned by non-DOD entities and considerably less of this infrastructure has been identified. DOD has not set a target date for identifying all of its non-DOD-owned critical infrastructure. DOD has determined that a small portion of the non-DOD-owned infrastructure—about 200 assets—that belongs to the defense industrial base defense sector is mission critical. Existing guidance requires various DOD components and sector lead agents to carry out the coordinated identification and assessment of critical infrastructure. Moreover, DOD components are pursuing varying approaches in identifying infrastructure critical to successfully carrying out its mission, which could make it difficult for DOD to make informed prioritization decisions and assess the effect of potential vulnerabilities across components and sector lead agents. Officials from several DOD components stated that a principal reason why the majority of critical infrastructure remains to be identified is because of the lack of timely guidance on identifying, prioritizing, and assessing critical infrastructure. DOD has recently begun to finalize this guidance. As DOD continues to identify its critical infrastructure, it also has been conducting a limited number of vulnerability assessments on DOD-owned assets. While these assessments can provide useful information about specific assets, until DOD identifies and prioritizes all of the critical infrastructure it owns, results have questionable value for

deciding where to target funding investments. In 2005, DOD incorporated an infrastructure assessment module into its existing antiterrorism vulnerability assessments, but has not made this approach a DOD-wide practice. DOD plans to implement a self-assessment program that would enable infrastructure owners to conduct additional vulnerability assessments, but guidance has not yet been issued. With the exception of critical infrastructure in the defense industrial base and transportation infrastructure supporting seaports and airports, DOD is not in a position to assess assets that it does not own; however, DOD does not have a mechanism to flag domestic mission-critical infrastructure for DHS to consider including among its assessments of the nation's critical infrastructure. DOD has delayed coordinating the assessment of non-DOD critical infrastructure located abroad while it focuses on identifying the infrastructure that it owns. Regarding current and future DCIP funding levels, including supplemental appropriations, the funding levels do not include the resources needed to remediate vulnerabilities that are identified through the assessments. As stated previously, our prior work has shown the importance of identifying all program costs to enable decision makers to weigh competing priorities. When DOD components and sector lead agents consistently identify, prioritize, and assess their critical infrastructure, as well as include the remediation of vulnerabilities in their funding requirements, DOD's ability to perform risk-based decision making and target funding to priority needs will be improved. We are recommending that DOD complete the identification and prioritization of critical infrastructure before increasing the number of infrastructure vulnerability assessments beyond current levels; adopt the practice of combining the infrastructure vulnerability assessment module with an existing assessment as the DOD-wide practice; expedite the issuance of guidance and criteria for performing infrastructure vulnerability self-assessments; flag domestic non-DOD-owned mission-critical infrastructure for DHS to consider including among its assessments of the nation's critical infrastructure; and identify funding for DCIP remediation.

GAO provided a draft of this report to DOD and DHS in April 2007 for their review and comment. In written comments on a draft of this report, DOD concurred with all of our recommendations. DHS had no comments. DOD also provided us with technical comments, which we incorporated in the report, as appropriate. DOD's response is reprinted in appendix II.

## Background

DOD recognizes that it is neither practical nor feasible to protect its entire infrastructure against every possible threat and, similar to DHS, it is pursuing a risk-management approach to prioritize resource and

operational requirements. Risk management is a systematic, analytical process to determine the likelihood that a threat will harm assets, and then to identify actions to reduce risk and mitigate the consequences of the threat. While risk generally cannot be eliminated, enhancing protection from threats or taking actions—such as establishing backup systems or hardening infrastructure—to reduce the effect of an incident can serve to significantly reduce risk.

DOD's risk-management approach is based on assessing threats, vulnerabilities, criticalities, and the ability to respond to incidents. Threat assessments identify and evaluate potential threats on the basis of capabilities, intentions, and past activities before they materialize. Vulnerability assessments identify weaknesses that may be exploited by identified threats and suggest options that address those weaknesses. For example, a vulnerability assessment might reveal weaknesses in unprotected infrastructure, such as satellites, bridges, and personnel records. Criticality assessments evaluate and prioritize assets on the basis of their importance to mission success. For example, certain power plants, computer networks, or population centers might be identified as important to the operation of a mission-critical seaport. These assessments help prioritize limited resources while reducing the potential for expending resources on lower-priority assets. DOD's risk-management approach also includes an assessment of the ability to respond to, and recover from, an incident.

The amount of non-DOD infrastructure that DOD relies on to carry out missions has not been identified; however, it is immense. To date, DHS has identified about 80,000 items of non-DOD infrastructure, some of which is also critical to DOD. Additionally, according to the Office of the Deputy Under Secretary of Defense for Installations and Environment, DOD owns more than 3,700 sites with more than half a million real property assets worldwide that could also qualify as critical infrastructure. The methodology DOD uses to identify critical infrastructure involves linking DOD missions to supporting critical infrastructure. Figure 2 shows three representative types of DOD-owned and non-DOD-owned critical infrastructure.

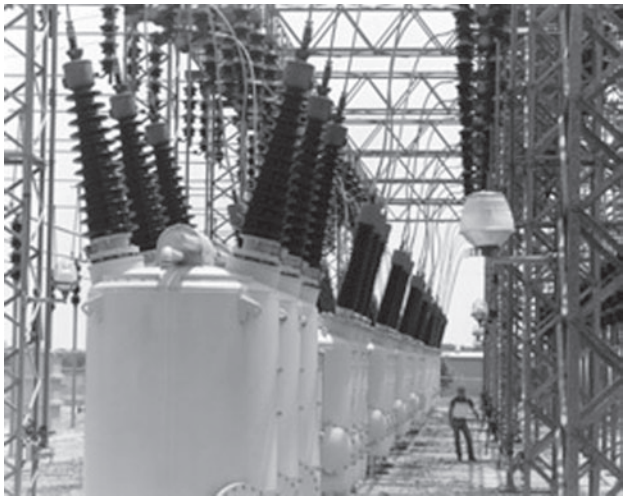
**Figure 2: Representative Types of Critical Infrastructure**

Source: DOD.

Sea-based radar system.

Source: DOD.

Hydroelectric dam.



Source: Department of Energy.

Power-generating plant switchyard.

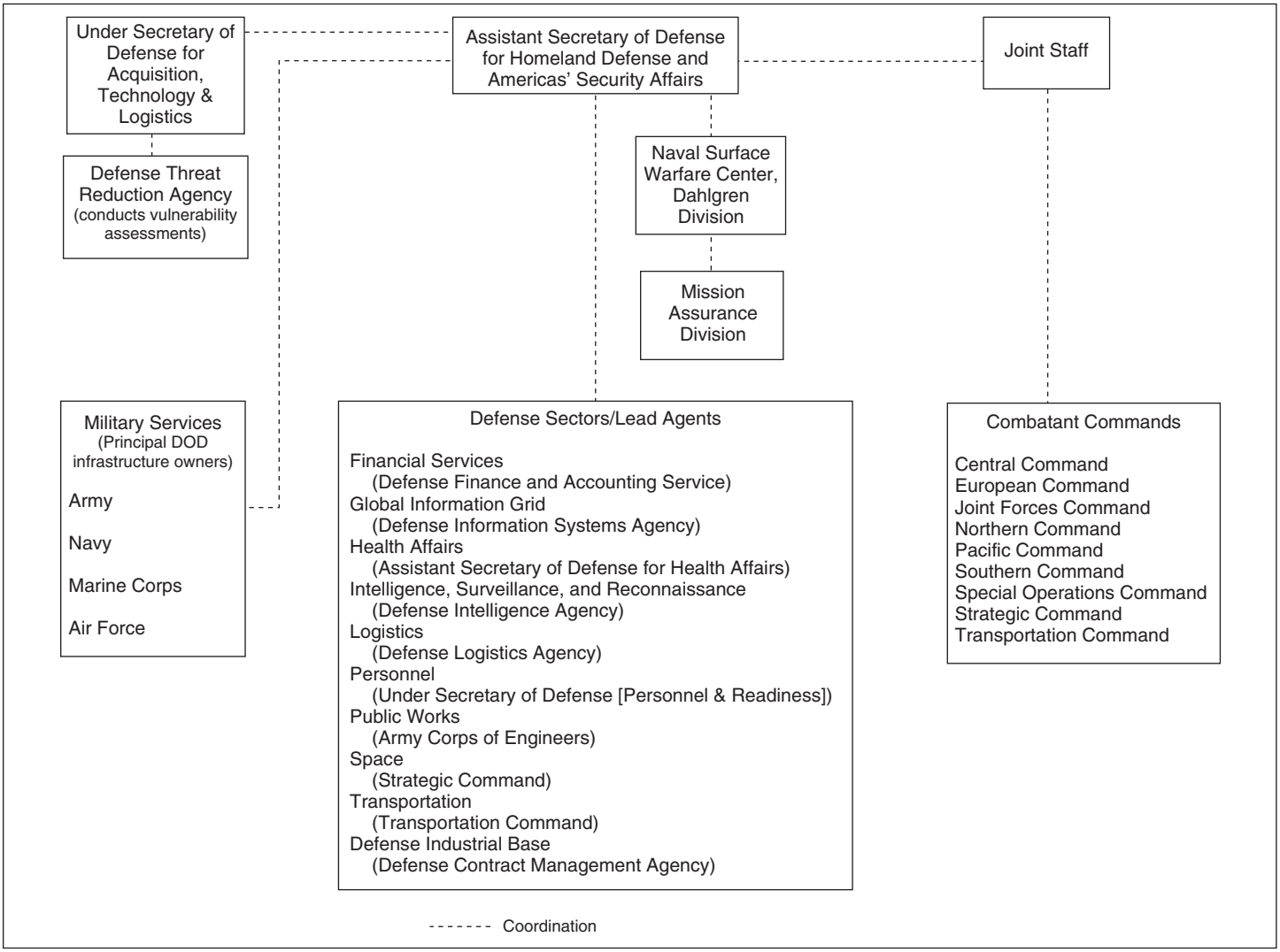
In 1998, the Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence was responsible for DOD's critical infrastructure protection efforts; however, in September 2003, the Deputy Secretary of Defense moved this program to the newly established

Office of the Assistant Secretary of Defense for Homeland Defense. DOD's critical infrastructure efforts were formalized in August 2005 with the issuance of DOD Directive 3020.40, which established DCIP. On December 13, 2006, this office was renamed the Office of the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs.

Shortly after the office became responsible for DOD's critical infrastructure protection efforts in October 2003, ASD(HD&ASA) established the Defense Program Office for Mission Assurance in Dahlgren, Virginia, to manage the day-to-day activities of DCIP. The Program Office—now a Mission Assurance Division—was responsible for coordinating DCIP efforts across DOD components and sector lead agents, developing training and exercise programs, overseeing the development of analytical tools and standards to permit DOD-wide analyses, and developing a comprehensive system to track and evaluate critical infrastructure.

DOD organizations that have significant DCIP roles and responsibilities are shown in figure 3.

**Figure 3: Key DOD DCIP Organizations**




Source: GAO analysis of DOD data.

The COCOMs, in collaboration with the Joint Staff, identify and prioritize DOD missions that are the basis for determining infrastructure criticality. The military services, as the principal owners of DOD infrastructure, identify and link infrastructure to specific COCOM mission requirements. Defense sector lead agents address the interdependencies among infrastructure that cross organizational boundaries, and evaluate the cascading effects of degraded or lost infrastructure on other infrastructure

assets. Further, DOD officials told us that DTRA performs infrastructure vulnerability assessments for the Joint Staff in support of DCIP to determine single points of failure from all hazards.

## DOD Has Taken Important Steps to Implement DCIP but Needs a Comprehensive Management Plan to Guide Its Efforts

DOD has taken some important steps to implement DCIP; however, it has not developed a comprehensive management plan to guide its efforts. Although an ASD(HD&ASA) official told us they are preparing an outline for a plan to implement DCIP, it is unclear the extent to which such a plan will address key elements associated with sound management practices, including issuing guidance, coordinating program stakeholders' efforts, and identifying resource requirements. DOD has been slow finalizing DCIP guidance and policies. As of May 2007, most of DOD's DCIP guidance and policies were either newly issued or still in draft, which has resulted in DOD's components pursuing varying approaches to implement DCIP. DOD has taken steps to improve information sharing and coordination within and outside of DOD. Finally, through DOD's budget process, DCIP has received over $160 million from fiscal years 2004 to 2007. Of this amount, the components and sector lead agents have received $68.6 million, of which about 21 percent is from supplemental appropriations. Our prior work has shown that supplemental funding is not an effective means for decision makers to effectively and efficiently plan for future years resource needs, weigh priorities, and assess budget trade-offs.[14] Until DOD completes a comprehensive management plan to implement DCIP, which includes issuing remaining DCIP guidance and fully identifying funding requirements, its ability to implement DCIP will be challenged.

### Most DCIP Guidance and Policies Are Newly Issued or Still in Draft

While our prior work has shown that issuing timely guidance is a key element of sound management, as of May 2007, the majority of DCIP guidance and policies were either newly issued or still in draft form, more than 3½ years after the Deputy Secretary of Defense assigned DCIP to ASD(HD&ASA) in September 2003 (see table 1).

[14]GAO has previously reported on DOD's overreliance on supplemental appropriations. See GAO, *Securing, Stabilizing, and Rebuilding Iraq: Key Issues for Congressional Oversight*, GAO-07-308SP (Washington, D.C.: Jan. 9, 2006); GAO, *Global War on Terrorism: Observations on Funding, Costs, and Future Commitments*, GAO-06-885T (Washington, D.C.: July 18, 2006); and GAO, *Force Structure: Actions Needed to Improve Estimates and Oversight of Costs for Transforming Army to a Modular Force*, GAO-05-926 (Washington, D.C.: Sept. 29, 2005).

**Table 1: Status of DCIP Guidance and Policies as of May 2007**

| Guidance document | Description | Status |
|---|---|---|
| *Critical Infrastructure Protection Security Classification Guide* | Establishes uniform criteria for classifying DCIP-related information to prevent its unauthorized disclosure. | Final, dated January 2003 |
| DOD Directive 3020.40, *Defense Critical Infrastructure Program (DCIP)* | Assigns responsibility for DCIP and incorporates guidance from Homeland Security Presidential Directive 7. | Final, dated August 19, 2005 |
| *DCIP Assessment Standards and Benchmarks* | Helps DOD components and sector lead agents determine vulnerabilities of their critical infrastructure and supporting foundational infrastructure. | Final, dated June 9, 2006 |
| *DCIP Geospatial Data Strategy* | Provides a common and comprehensive foundation for representing critical infrastructure geospatially. | Final, dated September 13, 2006 |
| *DCIP Criticality Process Guidance Document* | Provides a framework for identifying and prioritizing defense critical infrastructure. | Final, dated December 21, 2006 |
| *DCIP Data Collection Essential Elements of Information Data Sets* | Identifies required data elements DOD components and sector lead agents are to obtain on their critical infrastructure. | Draft, dated May 18, 2006 |
| *DCIP Interim Implementation Guidance* | Assigns responsibilities and prescribes DCIP procedures, and provides guidance to DOD components and sector lead agents on establishing their own critical infrastructure programs. | Final, dated July 13, 2006 |

Source: GAO analysis of DOD data.

In the absence of finalized guidance and policies, DOD components have been pursuing varying approaches to implement their critical infrastructure programs, a condition that has not changed markedly with the issuance of several guidance documents in the past year. According to officials responsible for the critical infrastructure programs from several of the DOD components, they were either unaware that the guidance had been finalized or had decided to continue the approach they had previously adopted.

Although DOD issued a DCIP directive in August 2005, ASD(HD&ASA) lacks a chartering directive that, among other things, clearly defines important roles, responsibilities, and relationships with other DOD organizations and missions—including the relationship between ASD(HD&ASA) and the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict and Interdependent Capabilities. At present, responsibility for antiterrorism guidance resides with the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict and Interdependent Capabilities. A memorandum entitled *Implementation Guidance Regarding the Office of the Assistant Secretary of Defense for Homeland Defense* issued by the Deputy Secretary of Defense in March 2003 required the Director of

Administration and Management within the Office of the Secretary of Defense to develop and coordinate within 45 days a chartering DOD Directive that would define, among other things, the relationship between ASD(HD&ASA) and the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict and Interdependent Capabilities. However, more than 4 years later, this chartering DOD directive still has not been accomplished.

Currently, DCIP implementation is diffused among program stakeholders, such as the COCOMs and the military services. As a consequence, some components, such as the U.S. Northern Command and U.S. Special Operations Command, leveraged DOD's antiterrorism guidance to develop critical infrastructure programs, while other components, such as the U.S. Strategic Command and U.S. European Command, have kept the two programs separate. Until DOD addresses the need for a chartering directive to properly identify the relationship between DCIP and the antiterrorism program, and sets timelines for finalizing its remaining guidance, it cannot be assured that components and sector lead agents identify, prioritize, and assess their critical infrastructure in a consistent manner. This lack of consistency could impair DOD's ability to perform risk-based decision making across component lines over the long term.

## Although DOD Has Taken Steps to Facilitate Information Sharing and Coordination, Additional Measures Could Be Taken

Existing DCIP guidance emphasizes information sharing and collaboration with relevant government and private-sector entities. While DOD has taken steps to facilitate information sharing and coordination within the department, as well as with other federal agencies and private sector companies, we believe additional measures could be taken, such as greater cooperation with federal-level counterparts on the identification, prioritization, and assessment of critical infrastructure. Since 2003, ASD(HD&ASA) has established and sponsored several information sharing and coordination forums, such as the Defense Infrastructure Sector Council and Critical Infrastructure Program Integration Staff. The Defense Infrastructure Sector Council provides a recurring forum for DCIP sector lead agents to share information, identify common areas of interest, and leverage the individual activities of each sector to eliminate duplication. The Critical Infrastructure Program Integration Staff is comprised of representatives from more than 30 DOD organizations. Additionally, ASD(HD&ASA) maintains an Internet site that is used to post relevant information, such as policies, available training, and announcement of meetings and conferences. ASD(HD&ASA) also is a member of several critical infrastructure forums whose membership extends beyond DOD, such as the Homeland Infrastructure Foundation Level Database Working

Group, and several Critical Infrastructure Partnership Advisory Council Committees, including those pertaining to communications, electricity, and dams. In another effort to coordinate DOD components' and sector lead agents' critical infrastructure protection practices, DOD released, in September 2006, its *DCIP Geospatial Data Strategy*, which lays out a standardized approach to depict geographically critical infrastructure data.

Both DHS and DOD officials acknowledged the potential benefits of increasing collaborative efforts, particularly with respect to critical infrastructure identification, tracking, and assessing. To promote clear and streamlined communication, ASD(HD&ASA) has directed DOD components and sector lead agents to channel their interactions with DHS through them. However, with the exception of the Health Affairs and Financial Services defense sectors, there has been little to no coordination between the defense sectors and their corresponding federal-level critical infrastructure sector counterparts due to the immaturity of the program. Table 2 shows the defense-level sectors that are comparable to those at the federal level.

**Table 2: Defense and Federal-Level Critical Infrastructure Sector Counterparts**

| Defense sector | Federal-level sector |
|---|---|
| Financial Services | Banking and Finance |
| Global Information Grid | Information Technology |
| | Telecommunications |
| Health Affairs | Public Health and Healthcare |
| | Agriculture and Food |
| Public Works | Dams |
| | Drinking Water and Water Treatment |
| Transportation | Transportation Systems |
| Defense Industrial Base | Defense Industrial Base |
| Intelligence, Surveillance, and Reconnaissance | No identified federal-level sector counterparts |
| Logistics | |
| Personnel | |
| Space | |
| No identified defense-sector counterparts | Chemical |
| | Commercial Facilities |
| | Commercial Nuclear Reactors, Materials, and Waste |
| | Emergency Services |
| | Energy |
| | Government Facilities |
| | National Monuments and Icons |
| | Postal and Shipping |

Source: DOD and DHS data.

DOD components are collecting different data to track and monitor their critical infrastructure to meet the needs of DCIP as well as their own, which could impede information sharing and analysis over time, and hinder DOD's ability to identify and prioritize critical infrastructure across DOD components and sector lead agents. ASD(HD&ASA) guidance on how DOD components and sector lead agents should track and monitor their critical infrastructure is in various stages of development and review. For example, in May 2006, ASD(HD&ASA) issued a draft version of the *DCIP Data Collection Essential Elements of Information Data Sets* requiring DOD components and sector lead agents to collect a common set of data on their critical infrastructure. However, officials from several of the COCOMs and defense sectors told us that they have not incorporated the *DCIP Data Collection Essential Elements of Information Data Sets* into their data collection efforts because the guidance has not been

finalized. These officials further stated that they are following departmental guidance[15] not specific to DCIP that pertains to database interoperability and data sharing. During fiscal year 2006, ASD(HD&ASA) tasked the Mission Assurance Division to develop the capability to geospatially display DOD components' and sector lead agents' critical infrastructure and interdependencies. The Mission Assurance Division has received and modeled critical infrastructure data from several defense sector lead agents, but according to division officials, the combination of funding constraints and the components and sector lead agents independently acquiring technical support for their individual critical infrastructure programs, has limited its utility.

In an effort to maximize the potential information DOD could receive about critical infrastructure it does not own, DOD officials told us that they plan to obtain Protected Critical Infrastructure Information (PCII) accreditation from DHS. The PCII program was established by DHS pursuant to the Critical Infrastructure Information Act of 2002.[16] The act provides that critical infrastructure information[17] that is voluntarily submitted to DHS[18] for use by DHS regarding the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other informational purpose, when accompanied with an express statement, shall receive various protections, including exemption from disclosure under the Freedom of Information Act.[19] If such information is validated by DHS as PCII, then the information can only be shared with authorized users.[20] Before accessing and storing

[15]See, for example, DOD Directive 8100.1, *Global Information Grid (GIG) Overarching Policy* (Washington, D.C.: Sept. 19, 2002) and DOD Directive 8320.2, *Data Sharing in a Net-Centric Department of Defense* (Washington, D.C.: Dec. 2, 2004).

[16]The Critical Infrastructure Information Act was enacted as Title II, Subtitle B of the Homeland Security Act of 2002, Pub. L. No. 107-296 (2002).

[17]"Critical infrastructure information" is defined at Section 212 of Pub. L. No. 107-296 (2002).

[18]DHS's final rule implementing the Critical Infrastructure Information Act identifies procedures for indirect submissions to DHS through DHS field representatives and other federal agencies.

[19]5 U.S.C. § 552.

[20]For more information on the procedures by which PCII may be shared, see DHS's *Procedures for Handling Critical Infrastructure Information*, 6 C.F.R. 29.

PCII, organizations or entities must be accredited and have a PCII officer.[21] Authorized users can request access to PCII on a need-to-know basis, but users outside of DHS do not have the authority to store PCII until their agency is accredited. However, the lack of accreditation does not otherwise prevent entities from sharing information directly with DOD. For example, in the aftermath of September 11, 2001, the Association of American Railroads began prioritizing railroad assets and vulnerabilities—information that it shares with DOD—on the more than 30,000 miles of commercial rail line used to transport defense critical assets.

DOD officials told us that DOD has not yet fully evaluated the costs and benefits of accreditation for its purposes. We noted in our April 2006 report that nonfederal entities continued to be reluctant to provide their sensitive information to DHS because they were not certain that their information will be fully protected, used for future legal or regulatory action, or inadvertently released. Since our April report,[22] DHS published on September 1, 2006, its final rule implementing the act, but we have not examined whether nonfederal entities are more willing to provide sensitive information to DHS under the act at this time, or DOD's cost to apply for, receive, and maintain accreditation. It is unclear to us, at this time, the extent to which obtaining accreditation would be beneficial to DOD when weighed against potential costs.

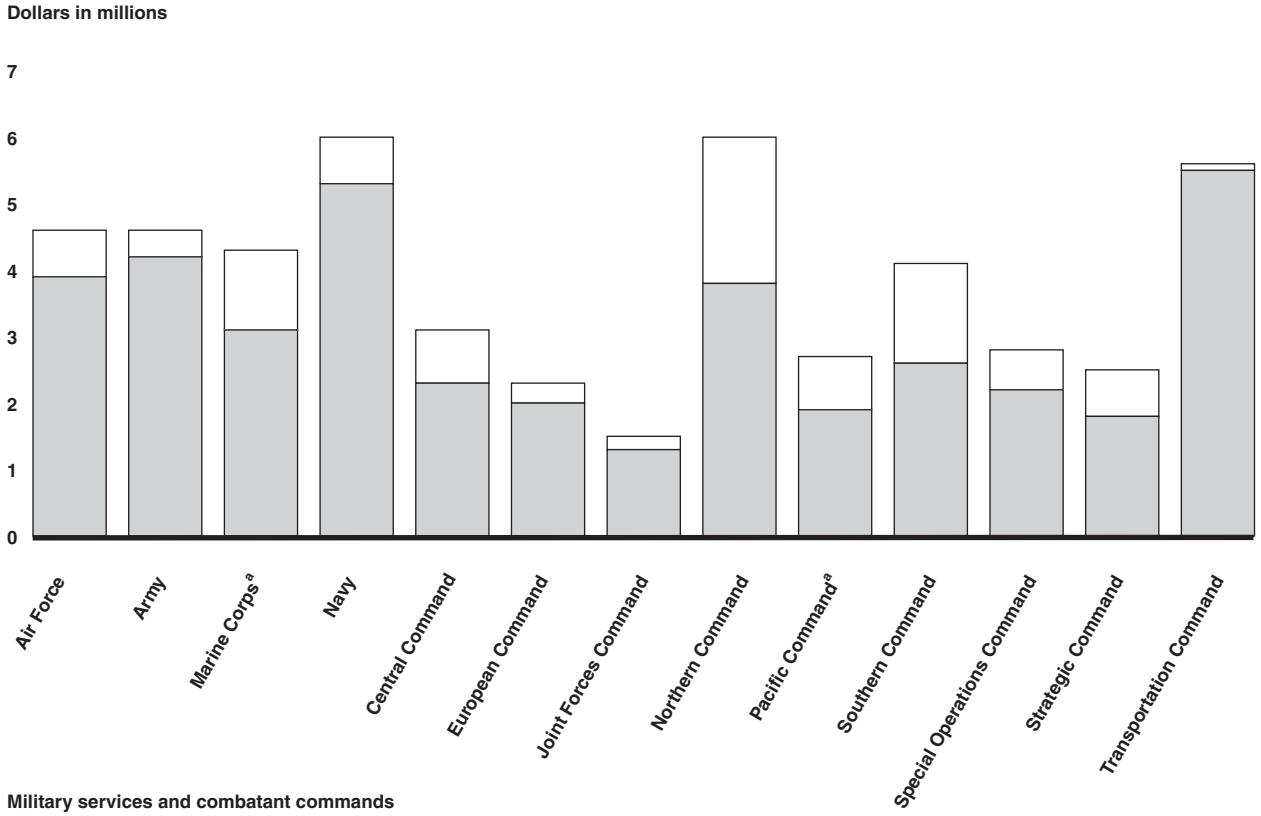
[21]For more information on the accreditation process, see app. II of GAO, *Information Sharing: DHS Should Take Steps to Encourage More Widespread Use of Its Program to Protect and Share Critical Infrastructure* Information, GAO-06-383 (Washington, D.C.: Apr. 17, 2006).

[22]GAO-06-383.

## DOD Components and Sector Lead Agents Have Relied on Supplemental Appropriations to Fund Their Critical Infrastructure Programs

DCIP has received about $160 million from fiscal years 2004 to 2007, through DOD's budget process. Of this amount, ASD(HD&ASA) received approximately $86.8 million, while the Joint Staff received approximately $5.3 million. The DOD components and sector lead agents, which are responsible for identifying critical infrastructure, received $68.5 million during the same 4-year period, of which $14.3 million (about 21 percent of the component and sector lead agents' combined funding) has come from supplemental appropriations. Figures 4 and 5 show how much DCIP funding was received by the components and sector lead agents during fiscal years 2004 to 2007.

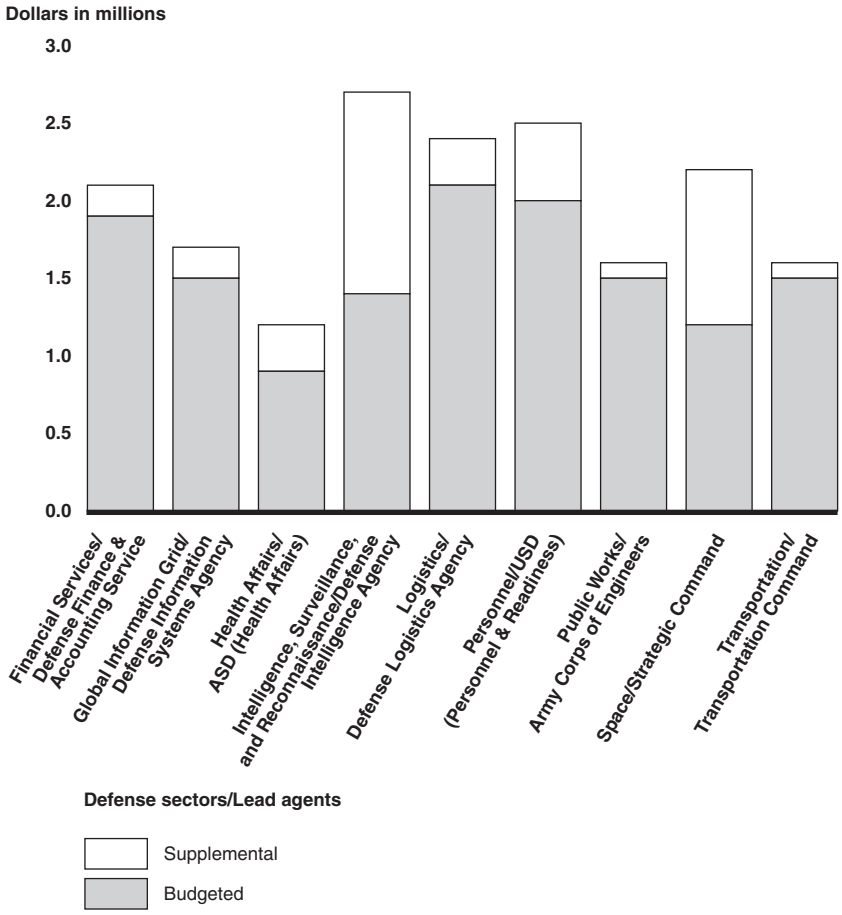
**Figure 4: Total DCIP Funding by Military Service and COCOM, Fiscal Years 2004 to 2007**




Source: GAO analysis of DOD data.

[a]The Marine Corps and U.S. Pacific Command totals do not include funding for fiscal year 2004 because these data were unavailable.

**Figure 5: Total DCIP Funding by Defense Sector, Fiscal Years 2004 to 2007**




Source: GAO analysis of DOD data.

Note: The $6.8 million provided to the Defense Contract Management Agency, the Defense Sector Lead Agent for the Defense Industrial Base, is not included.

The extent to which individual components and sector lead agents relied on supplemental funding for their critical infrastructure programs varied by fiscal year. In fiscal year 2005, for example, both the U.S. Special Operations Command and the Health Affairs defense sector did not receive any programmed funding and relied exclusively on supplemental appropriations. The Defense Intelligence Agency, the lead agent for the Intelligence, Surveillance, and Reconnaissance defense sector, received 78 percent of its fiscal year 2005 critical infrastructure funding from supplemental appropriations. Likewise, the U.S. Northern Command received almost three-quarters (72 percent) of its critical infrastructure funding from supplemental appropriations in fiscal year 2006. Management

control standards contained in the *Standards for Internal Control in the Federal Government* and sound management practices emphasize the importance of effective and efficient resource use. Relying on supplemental funding to varying degrees for their DCIP budget prevents the components and sector lead agents from effectively planning future years' resource needs, weighing priorities, and assessing budget trade-offs.

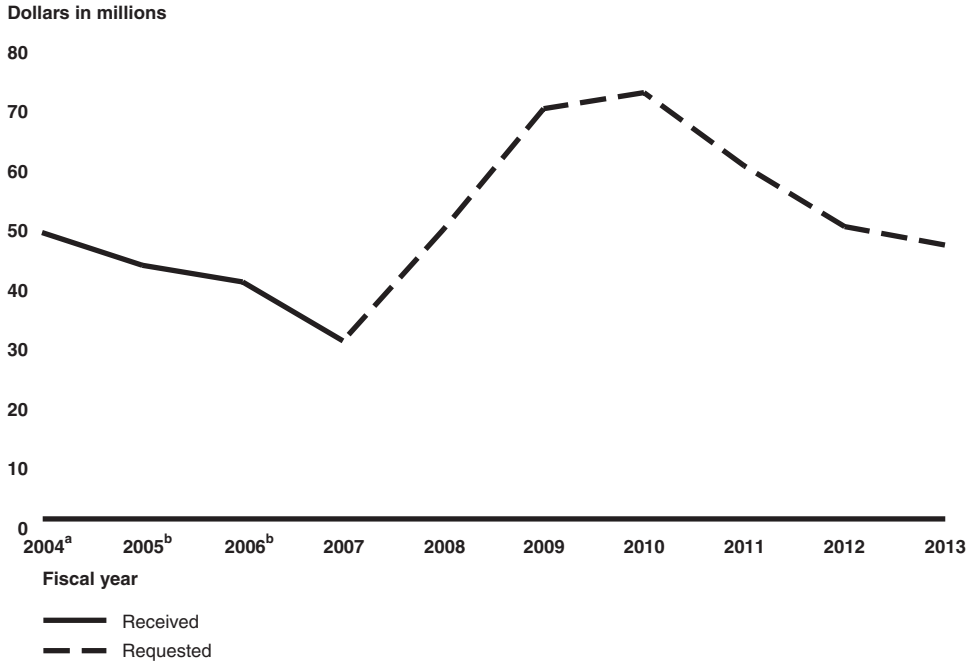
DCIP funding has been centralized in ASD(HD&ASA) since fiscal year 2004; however, beginning in fiscal year 2008, the military departments will be required to fund service critical infrastructure programs as well as the nine COCOM critical infrastructure programs. According to DOD Directive 3020.40,[23] the military departments and COCOMs are required to provide resources for programs supporting DCIP. This responsibility is reiterated and amplified in a memorandum[24] from the Principal Deputy Assistant Secretary of Defense for Homeland Defense that instructs the military departments and the COCOMs to include DCIP funding in their fiscal year 2008 to 2013 budget submissions. ASD(HD&ASA) will continue to fund defense sector critical infrastructure programs for fiscal years 2008 and 2009, and ASD(HD&ASA) officials stated that they will work with the defense sector lead agents to obtain funding through the lead agents' regular budget process, beginning in fiscal year 2010. Including DCIP in the lead agents' baseline budgets should reduce reliance on supplemental appropriations to implement critical infrastructure responsibilities.

Overall DCIP funding received (fiscal years 2004 to 2007), and requested (fiscal years 2008 to 2013) is shown in figure 6.

[23]DOD Directive 3020.40 states that the COCOMs are to identify an office of primary responsibility to establish, resource, and execute a command program for matters pertaining to the identification, prioritization, and protection of command mission essential tasks and required capabilities, and the military services are to establish, resource, and execute an organizational program supporting DCIP.

[24]See Memorandum on *Defense Critical Infrastructure Program Funding Responsibilities* from the Principal Deputy Assistant Secretary of Defense for Homeland Defense dated February 15, 2006.

**Figure 6: DCIP Funding for Fiscal Years 2004 to 2013**




Source: GAO analysis of ASD(HD&ASA) data.

Note: Funding for the Defense Industrial Base defense sector is not included.

[a]DCIP funding for fiscal year 2004 does not include funding for the Marine Corps or the U.S. Pacific Command because these data were unavailable.

[b]DCIP funding includes supplemental funding received in fiscal years 2005 and 2006.

If DCIP is funded at requested levels in future years, then it will represent a substantial increase over current actual funding levels. However, in previous years, DCIP consistently has been funded at less than the requested amounts. For example, in fiscal year 2005, the military services collectively requested approximately $8 million in DCIP funding from ASD(HD&ASA) and received $2.1 million. That year, the military services also received an additional $2.3 million in supplemental appropriations, raising their total funding in fiscal year 2005 to $4.4 million, which is approximately 55 percent of what was requested. Even if DCIP funding is substantially increased, without a comprehensive management plan in place, it is not clear that the funds would be allocated to priority needs.

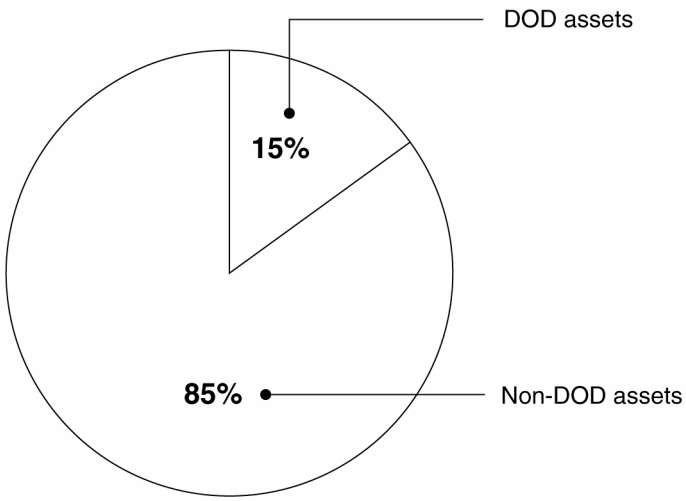
## DOD Estimates That It Has Identified about 25 Percent of the Critical Infrastructure It Owns, and Most of the Non-DOD-Owned Critical Infrastructure Remains Unidentified

DOD estimates that it has identified about 25 percent of the critical infrastructure it owns, and expects to finish identifying the remaining 75 percent by the end of fiscal year 2009. DOD has identified considerably less of its critical infrastructure owned by non-DOD entities, and has not set a target date for its completion. A principal reason why DOD has not identified a greater amount of its critical infrastructure is the lack of timely DCIP guidance and policies, which has resulted in DOD's components pursuing varying approaches in identifying their critical infrastructure. DOD has been performing a limited number of vulnerability assessments on DOD-owned infrastructure; however, until DOD identifies and prioritizes all of the critical infrastructure it owns, results have questionable value for deciding where to target funding investments. Currently, DOD includes the vulnerability assessment of DOD-owned infrastructure as a module to an existing assessment. However, it has not formally adopted this practice DOD-wide, which would reduce the burden on installation personnel and asset owners. Moreover, DOD does not have a mechanism to flag domestic mission-critical infrastructure for DHS to consider including among its assessments of the nation's critical infrastructure, and has delayed coordinating the assessments of non-DOD critical infrastructure located abroad. DOD has not identified funding to remediate vulnerabilities identified through the assessment process.

### DOD Has Identified Some of Its Mission-Critical Infrastructure

DOD estimates that it has identified about 25 percent of the critical infrastructure it owns, and ASD(HD&ASA) officials anticipate identifying all DOD-owned critical infrastructure (estimated to be about 15 percent of the total) by the fiscal year 2008–2009 time frame. DOD has identified considerably less critical infrastructure that it does not own (estimated to be about 85 percent of the total), but that it relies upon to perform its missions (see fig. 7).

**Figure 7: Allocation of Critical Infrastructure DOD Owns and Does Not Own**




Source: GAO analysis of DOD data.

Without knowing how much non-DOD-owned infrastructure is mission critical, ASD(HD&ASA) officials were unable to estimate how much of the non-DOD infrastructure has already been identified or a completion date. DOD has determined that a small portion of the non-DOD infrastructure—about 200 assets—that belongs to the defense industrial base sector are mission critical.

The Mission Assurance Division developed a database to track and geospatially display defense critical infrastructure both within the United States and overseas, and its associated interdependencies. According to Mission Assurance Division officials, the willingness of DOD components to share their critical infrastructure information has varied. For example, division officials told us that the defense sectors have been more forthcoming than either the military services or the COCOMs. Consequently, the database provides an incomplete view of defense critical infrastructure, which significantly reduces DOD's ability to analyze the importance of infrastructure across the components and sector lead agents. ASD(HD&ASA) officials are aware that several of the DOD components and sector lead agents have developed databases to track their specific infrastructure. For example, the Air Force, Marine Corps, Health Affairs sector, Space sector and Personnel sector have each developed their own databases. According to ASD(HD&ASA) officials, they are focusing on ensuring compatibility among the databases rather

than prescribing a central database. Until DOD identifies the remaining portion of its critical infrastructure, including the portion owned by non-DOD entities, it cannot accurately prioritize and assess the risks associated with that infrastructure.

Table 3 shows the amount of infrastructure assets—rounded to the nearest hundred—that the DOD components have provisionally identified as critical as of December 2006. DOD officials cautioned that not all of this information has been validated and is subject to change. For example, some infrastructure may be counted more than once due to components performing multiple missions or being assigned dual roles. The numbers in table 3 are presented to provide an order of magnitude.

**Table 3: DOD-Owned Infrastructure Provisionally Identified as Critical**

| DOD component | Critical infrastructure assets identified |
|---|---|
| Military services | 3,400 |
| COCOMs[a] | 900 |
| Defense sector lead agents | 1,600 |
| **Total** | **5,900** |

Source: GAO's analysis of DOD data.

[a]The U.S. Strategic Command and the U.S. Transportation Command have dual roles as combatant commands and defense sector lead agents. Their identified critical infrastructure is included in the COCOM total.

According to the *Standards for Internal Control in the Federal Government*, appropriate policies and procedures should exist with respect to an agency's planning and implementation activities. The length of time DOD has taken to issue DCIP guidance and policies has resulted in components pursuing varying approaches in identifying and prioritizing critical infrastructure, approaches that may not be complementary. For example, Navy officials told us that, prior to 2004, they were basing infrastructure criticality on its importance to Operation Enduring Freedom, whereas Army officials indicated that they are using wartime planning scenarios based on the 2006 Quadrennial Defense Review to determine criticality. The COCOMs and the Joint Staff are basing infrastructure criticality on its importance in accomplishing individual COCOM mission requirements—an idea proposed by the Mission Assurance Division. In 2003, the Mission Assurance Division proposed linking infrastructure criticality with COCOM mission requirements, and Joint Staff officials stated that a preliminary list has been formulated and will undergo further review in 2007. Furthermore, defense sector lead

agents, such as Financial Services and Personnel, are identifying all of their infrastructure regardless of COCOM mission requirements. These variations in approaches used to determine criticality exist because DOD's published policy, the *DCIP Criticality Process Guidance Document*, which directs the components and sector lead agents to use one set of criteria—COCOM mission requirements—was not finalized until December 2006.

## Vulnerability Assessments of DOD-Owned Infrastructure Have Limited Value without Knowing Infrastructure Criticality, and DOD Would Benefit from Formally Adopting a Departmentwide Practice, and Flagging Non-DOD-Owned Infrastructure for DHS's Consideration

DOD has begun conducting a limited number of infrastructure vulnerability assessments on the infrastructure it owns. Between calendar years 2004 and 2007, DTRA will have conducted approximately 361 antiterrorism vulnerability assessments, 45 (about 12 percent) of which will include an assessment of critical infrastructure. Which installations receive antiterrorism vulnerability assessments with a module that focuses on critical infrastructure is based on perceived infrastructure criticality, as determined by the Joint Staff in coordination with the COCOMs, and to a lesser extent the military services. However, we believe DOD cannot effectively target infrastructure vulnerability assessments without first identifying and prioritizing its mission-critical infrastructure. Depending on the amount of infrastructure that DOD deems critical, it may not be able to perform an on-site assessment of every DOD asset. To address this limitation, ASD(HD&ASA) officials told us that they plan to implement a self-assessment program that the military services—the infrastructure owners—can conduct in lieu of or in between the scheduled vulnerability assessments. DOD is in the process of developing a vulnerability self-assessment handbook that would provide guidance on how to conduct these assessments but, as of May 2007, a release date had not been set.

To reduce the burden of multiple assessments on installation personnel and asset owners, in 2005, DOD incorporated an all-hazards infrastructure assessment module into its existing antiterrorism vulnerability assessments. Including the vulnerability assessment of DOD infrastructure in an established assessment program, such as the one that exists for antiterrorism, has not been formally adopted as a departmentwide practice. Unless this practice is adopted, it is possible that infrastructure assessments could be conducted independently, thereby increasing the burden on installation personnel and asset owners that the modular approach alleviates. Beginning in calendar year 2006, the Air Force piloted its own critical infrastructure assessments at those Air Force installations not receiving DTRA-led vulnerability assessments. The Air Force completed two of these pilot critical infrastructure assessments in 2006, and has nine additional assessments planned in 2007. Unlike the DTRA-led

assessments, the Air Force pilot assessments are based on risk rather than vulnerabilities. We did not examine the quality or the sources of the threat, asset criticality, and vulnerability data that the Air Force is using to perform its risk assessments. We did not evaluate the effectiveness of either the DTRA-led or Air Force assessments as part of our review.

DOD is not in a position to address domestic, non-DOD, mission-critical infrastructure, with the exception of defense industrial base assets and transportation infrastructure supporting seaports and airports, much less perform vulnerability assessments on them. DHS conducts on-site vulnerability assessments of domestic non-DOD-owned critical infrastructure and has developed a model that enables owners of private-sector critical infrastructure to perform vulnerability self-assessments. DOD currently does not have a mechanism to flag mission-critical infrastructure for DHS to consider including among its assessments of the nation's critical infrastructure. For example, if DOD knew that DHS was planning to conduct a vulnerability assessment of critical infrastructure in the Atlanta, Georgia, area, it could flag for DHS's consideration privately-owned infrastructure that DOD deemed critical—such as an electrical substation or a railroad junction. Officials from both agencies expressed an interest in coordinating vulnerability assessments of non-DOD-owned critical infrastructure. DOD has delayed coordinating the assessments of non-DOD-owned infrastructure located abroad because it has decided to focus on identifying infrastructure that it owns. For example, U.S. European Command and U.S. Central Command officials stated that they are concentrating on identifying critical infrastructure located on their installations. In addition, DTRA officials pointed out that gaining access to relevant information about foreign-owned infrastructure is more challenging than for infrastructure owned domestically.

## DCIP Funding Requirements Do Not Include Remediation

Future DCIP funding requests may be understated because current funding levels, including supplemental appropriations, do not include the resources that may be needed to remediate vulnerabilities. Our prior work has shown the importance of identifying all program costs to enable decision makers to weigh competing priorities. According to critical infrastructure officials from several DOD components and sector lead agents, there is insufficient funding to remediate vulnerabilities identified through the assessment process. Remediation in the form of added protective measures, backup systems, hardening infrastructure against perceived threats, and building redundancy could be costly. As a point of reference, the Joint Staff spent $233.7 million from fiscal years 2004

through 2007 to correct high-priority antiterrorism vulnerabilities—more than the $160 million spent on all DCIP activities over this same period.

Additionally, these antiterrorism remediation expenditures were for DOD-owned assets only and do not reflect costs to remediate vulnerabilities to infrastructure not owned by DOD. In 2000, the Congress directed the Secretary of Defense to establish a loan guarantee program[25] that makes a maximum of $10 million loan principal guarantee available each fiscal year for qualified commercial firms to improve the protection of their critical infrastructure at their facilities or refinance improvements previously made. Once DOD identifies the critical infrastructure it relies on but does not own and its associated vulnerabilities, this program could potentially be utilized to help qualified commercial firms obtain funding for remediation.

## Conclusions

DOD depends on critical infrastructure to project, support, and sustain its forces and operations worldwide, but its lack of a comprehensive management plan to guide its efforts that addresses guidance, coordination of program stakeholders' efforts, and resource requirements, has prevented the department from effectively implementing an efficient critical infrastructure program. ASD(HD&ASA) has overseen DCIP since September 2003; however, because key DCIP guidance has either recently been issued or remains in draft more than 3½ years later, DOD components have been pursuing different approaches to fulfill their DCIP missions—approaches that are not optimally coordinated and may conflict with each other or their federal-level counterparts. Moreover, because the relationship between the Directorates for HD&ASA and Special Operations and Low-Intensity Conflict and Interdependent Capabilities regarding the DCIP and antiterrorism missions remains undefined, some components are relying on antiterrorism guidance to implement their critical infrastructure programs while others take different approaches. Furthermore, some DCIP funding for the components and sector lead agents has come from supplemental appropriations, which, as we have reported previously, is not a reliable means for decision makers to effectively and efficiently assess resource needs. Until DOD develops a comprehensive management plan for DCIP—that includes timelines for finalizing remaining guidance and actions to improve information sharing, its ability to implement DCIP will be challenged.

[25]Pub. L. No. 106-398 § 1033 (2000), codified at 10 U.S.C. § 2541.

In addition, until DOD identifies and prioritizes what infrastructure is critical, the utility of vulnerability assessments is limited in targeting funding and investments and could lead to an inefficient use of DOD resources. Combining the infrastructure vulnerability assessment with an existing assessment, as DOD is currently doing on infrastructure that it owns, has the added advantage of reducing the burden of multiple assessments on installation personnel and asset owners. However, because DOD has not formally adopted this modular approach as a DOD-wide practice, the possibility exists that infrastructure vulnerability could be assessed separately. Still, to date, no DCIP funds have been spent on reducing vulnerabilities to infrastructure. Remediation of risk identified in the assessment process could be costly—possibly more than doubling current identified funding requirements. Finally, by not coordinating with DHS on vulnerability assessments of non-DOD domestic infrastructure, DOD is missing an opportunity to increase awareness of matters affecting the availability of assets that it relies on but does not control. When DOD components and sector lead agents consistently identify, prioritize, and assess their critical infrastructure, as well as including the remediation of vulnerabilities in their funding requirements, DOD's ability to perform risk-based decision making and target funding to priority needs will be improved.

## Recommendations for Executive Action

To guide DCIP implementation, we recommend that the Secretary of Defense direct ASD(HD&ASA) to develop and implement a comprehensive management plan that addresses guidance, coordination of stakeholders' efforts, and resources needed to implement DCIP. Such a plan should include establishing timelines for finalizing the DCIP *Data Collection Essential Elements of Information Data Sets* to enhance the likelihood that DOD components and sector lead agents will take a consistent approach in implementing DCIP.

To implement the intent of the Deputy Secretary of Defense's memorandum *Implementation Guidance Regarding the Office of the Assistant Secretary of Defense for Homeland Defense* dated March 25, 2003, we recommend that the Secretary of Defense direct the Director of Administration and Management to issue a chartering directive to, among other things, define the relationship between the Directorates for HD&ASA and Special Operations and Low-Intensity Conflict and Interdependent Capabilities.

As part of this comprehensive management plan, to increase the likelihood that the defense sector lead agents are able to make effective budgetary

decisions, we recommend that the Secretary of Defense direct ASD(HD&ASA) to assist the defense sector lead agents in identifying, prioritizing, and including DCIP funding requirements through the regular budgeting process beginning in fiscal year 2010.

In addition, as part of developing a comprehensive management plan for DCIP, we recommend that the Secretary of Defense direct ASD(HD&ASA), in coordination with the DOD components and sector lead agents, to determine funding levels and sources needed to avoid reliance on supplemental appropriations and identify funding for DCIP remediation.

We further recommend that the Secretary of Defense direct ASD(HD&ASA) to take the following actions to increase the utility of vulnerability assessments:

- Complete the identification and prioritization of critical infrastructure before increasing the number of infrastructure vulnerability assessments performed.
- Adopt the practice of combining the defense critical infrastructure vulnerability assessment module with an existing assessment as the DOD-wide practice.
- Issue guidance and criteria for performing infrastructure vulnerability self-assessments.
- Identify and prioritize domestic non-DOD-owned critical infrastructure for DHS to consider including among its assessments of the nation's critical infrastructure.

## Agency Comments and Our Evaluation

In written comments on a draft of this report, DOD concurred with all of our recommendations. DOD also provided us with technical comments, which we incorporated in the report, as appropriate. DOD's comments are reprinted in appendix II. DHS also was provided with an opportunity to comment on a draft of this report, but informed us that it had no comments.

In its written comments, DOD stated that it expects to issue its DCIP management plan by September 2007 and a chartering directive for ASD(HD&ASA) by July 2007—guidance that we believe will contribute to a more efficient and effective critical infrastructure program. Although DOD did not describe the contents of the management plan, we encourage the department to address points raised in our report—guidance, coordination of stakeholders' efforts, and resource requirements. DOD concurred with our recommendations pertaining to infrastructure

vulnerability assessments. Specifically, it agreed to identify and prioritize all DOD-owned critical infrastructure before increasing the number of assessments; to codify the practice of combining the infrastructure assessment with an existing vulnerability assessment, thereby reducing the burden of multiple assessments on installation personnel and asset owners; and to issue self-assessment guidance and criteria. In its comments, DOD stated that vulnerability assessments are a valid tool to address risk and support risk management decisions, and that delaying these assessments until all assets are identified—projected in fiscal year 2009—is unadvisable. While we agree that infrastructure vulnerability assessments can reveal exploitable weaknesses, without evaluating the capabilities, intentions, or probability of occurrence of human and natural threats, as well as the importance of a particular asset to accomplishing the mission, reducing vulnerabilities may result in little, if any, risk reduction. We agree with the department that it should continue to perform infrastructure vulnerability assessments, but believe that increasing the number of assessments performed above current levels will have limited value without considering threat and asset criticality. With respect to our recommendation on vulnerability self-assessments, DOD's expectation that installation personnel and asset owners have the expertise and resources to apply standards and criteria that mirror what DTRA is using to perform its DCIP vulnerability assessments may be unrealistic. We believe that DOD's earlier approach of preparing a self-assessment handbook tailored to meet a range of installation and asset requirements and capabilities will likely result in more and higher-quality self-assessments. DOD also agreed with our recommendation to identify and prioritize non-DOD-owned domestic infrastructure for DHS to consider including among its assessments of the nation's critical infrastructure. We expect that this action will increase DOD's awareness of vulnerabilities associated with infrastructure that it relies on but does not control.

As agreed with your offices, we are sending copies of this report to the Chairman and Ranking Member of the Senate and House Committees on Appropriations, Senate and House Committees on Armed Services, and other interested congressional parties. We also are sending copies of this report to the Secretary of Defense; the Secretary of Homeland Security; the Director, Office of Management and Budget; and the Chairman of the Joint Chiefs of Staff. We will also make copies available to others upon request. In addition, this report will be available at no charge on the GAO Web site at http://www.gao.gov.

If you or your staff have any questions concerning this report, please contact me at (202) 512-5431 or by e-mail at dagostinod@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix III.

Davi M. D'Agostino
Director, Defense Capabilities and
Management

# Appendix I: Scope and Methodology

To conduct our review of the Department of Defense's (DOD) Defense Critical Infrastructure Program (DCIP), we obtained relevant documentation and interviewed officials from the following DOD organizations:[1]

- Office of the Secretary of Defense
  - Under Secretary of Defense for Personnel and Readiness, Information Technology Division;
  - Under Secretary of Defense for Acquisition, Technology, and Logistics, Office of the Deputy Under Secretary of Defense for Industrial Policy;
  - Under Secretary of Defense for Intelligence, Counterintelligence & Security, Physical Security Programs;
    - DOD Counterintelligence Field Activity, Critical Infrastructure Protection Program Management Directorate;
  - Under Secretary of Defense (Comptroller)/Chief Financial Officer;
  - Deputy Under Secretary of Defense for Installations and Environment, Business Enterprise Integration Directorate;
  - Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs (ASD[HD&ASA]), Critical Infrastructure Protection Office;
  - Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict and Interdependent Capabilities, Antiterrorism Policy;
  - Assistant Secretary of Defense for International Security Policy, Deputy Assistant Secretary of Defense for Forces Policy, Office of Space Policy;
  - Assistant Secretary of Defense for Health Affairs, Force Health Protection & Readiness; and
  - Assistant Secretary of Defense for Networks and Information Integration, Information Management & Technology Directorate;
- Joint Staff, Directorate for Operations, Antiterrorism and Homeland Defense
- Defense Threat Reduction Agency (DTRA), Combat Support Assessments Division
- Military Services
  - Department of the Army, Asymmetric Warfare Office, Critical Infrastructure Risk Management Branch;
  - Department of the Navy
    - Office of the Chief Information Officer;

[1]DOD organizations are located in the Washington, D.C., metropolitan area unless indicated otherwise.

    - Mission Assurance Division, Naval Surface Warfare Center, Dahlgren Division, Dahlgren, Virginia;
  - Department of the Air Force, Air, Space and Information Operations, Plans, and Requirements, Homeland Defense Division; and
  - Headquarters, U.S. Marine Corps, Security Division, Critical Infrastructure Protection Office;
- Combatant Commands
  - Headquarters, U.S. Central Command, Defense Critical Infrastructure Program Office, MacDill Air Force Base, Florida;
  - Headquarters, U.S. European Command, Critical Infrastructure Protection Program Office, Patch Barracks, Germany;
  - Headquarters, U.S. Joint Forces Command, Critical Infrastructure Protection Office, Norfolk, Virginia;
  - Headquarters, U.S. Northern Command, Force Protection/Mission Assurance Division, Peterson Air Force Base, Colorado;
  - Headquarters, U.S. Pacific Command, Critical Infrastructure Protection Plans & Policy Office, Camp H.M. Smith, Hawaii;
  - Headquarters, U.S. Southern Command, Joint Operations Support Division, Miami, Florida;
  - Headquarters, U.S. Special Operations Command, Mission Assurance Division, MacDill Air Force Base, Florida;
  - Headquarters, U.S. Strategic Command, Mission Assurance Division, Offutt Air Force Base, Nebraska; and
  - Headquarters, U.S. Transportation Command, Critical Infrastructure Program, Scott Air Force Base, Illinois;
- Defense Sector Lead Agents
  - Headquarters, Defense Intelligence Agency, Office for Critical Infrastructure Protection & Homeland Security/Defense;
  - Headquarters, Defense Information Systems Agency, Critical Infrastructure Protection Team;
  - Headquarters, Defense Finance and Accounting Service, Critical Infrastructure Protection Program Office, Indianapolis, Indiana;
  - Headquarters, Defense Logistics Agency, Logistics Sector Critical Infrastructure Protection Office;
  - Headquarters, U.S. Army Corps of Engineers, Directorate of Military Programs;
  - Under Secretary of Defense for Personnel and Readiness, Information Technology Division;
  - Assistant Secretary of Defense for Health Affairs, Directorate of Force Health Protection & Readiness;
  - Headquarters, U.S. Transportation Command, Critical Infrastructure Program, Operations Directorate, Scott Air Force Base, Illinois; and

- Headquarters, U.S. Strategic Command, Mission Assurance Division, Offutt Air Force Base, Nebraska.

To evaluate the extent to which DOD has developed a comprehensive management plan to implement DCIP, we reviewed and analyzed policies, assurance plans, strategies, handbooks, directives, and instructions, and met with officials from each of the military services, combatant commands (COCOM) (hereafter referred to as "DOD components"), and the defense sector lead agents, as well as the Joint Staff. We compared DOD's current approach to issuing guidance, stakeholder coordination, and resource requirements to management control standards contained in the *Standards for Internal Control in the Federal Government*. We also attended the August 2006 DCIP tabletop exercise sponsored by the Defense Intelligence Agency, and the October 2006 Homeland Infrastructure Foundation Level Database Working Group meeting. We met with representatives from ASD(HD&ASA), the Joint Staff, and several offices within the Office of the Secretary of Defense assigned DCIP responsibilities in DOD Directive 3020.40, *Defense Critical Infrastructure Protection (DCIP)*, as well as the Office of the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict and Interdependent Capabilities. Further, we met with officials from the Department of Homeland Security's (DHS) Office of Infrastructure Protection to discuss mechanisms to coordinate and share critical infrastructure information with DOD.

To determine DCIP funding levels for fiscal years 2004 through 2013, we met with officials from ASD(HD&ASA) and each of the DOD components and sector lead agents, and analyzed actual and projected funding data. We also met with an official from the Office of the Under Secretary of Defense (Comptroller)/Chief Financial Officer familiar with DCIP. Additionally, we obtained information from the Joint Staff on funds expended to remediate high-priority antiterrorism vulnerabilities to illustrate the potential cost of critical infrastructure remediation. We found the data provided by DOD to be sufficiently reliable for representing the nature and extent of DCIP funding.

To evaluate the extent to which DOD has identified, prioritized, and assessed its critical infrastructure, we met with officials and obtained relevant documentation from each of the DOD components, sector lead agents, ASD(HD&ASA), the Joint Staff, and the Mission Assurance Division. We examined various data collection instruments and databases DOD components and sector lead agents are using to catalog, track, and map infrastructure, including the Mission Assurance Division's database,

the Air Force's Critical Asset Management System, the Health Affairs defense sector's Primary Health Assets Staging Tool, the Personnel defense sector's Characterization and Dependency Analysis Tool, and the Space defense sector's Strategic Mission Assurance Data System. We also received a demonstration of DHS's National Asset Database, which catalogs the nation's infrastructure. We did not verify the accuracy of infrastructure provisionally identified as critical by the DOD components and sector lead agents because the data is incomplete and, has not been validated by the department. Further, we did not verify the interoperability of these databases because it was outside the scope of our review. We met with DTRA officials to obtain information on the scope, conduct, and results of infrastructure vulnerability assessments. We also met with Air Force officials to discuss their infrastructure risk assessments. We did not evaluate the effectiveness of either the DTRA-led or Air Force assessments as part of our review.

Finally, to become familiar with prior work relevant to defense critical infrastructure, we met in Arlington, Virginia, with officials from the George Mason University School of Law's Critical Infrastructure Protection Program and in Washington, D.C., with the Congressional Research Service (Resources, Science, and Industry Division and Foreign Affairs, Defense, and Trade Division).

We conducted our review from June 2006 through May 2007 in accordance with generally accepted government auditing standards.

# Appendix II: Comments from the Department of Defense

ASSISTANT SECRETARY OF DEFENSE
2600 DEFENSE PENTAGON
WASHINGTON, DC 20301-2600

HOMELAND DEFENSE

MAY 1 5 2007

Ms. Davi M. D'Agostino
Director, Defense Capabilities and Management
U.S. Government Accountability Office
441 G Street, N.W.
Washington, DC 20548

Dear Ms. D'Agostino:

Enclosed is the Department of Defense (DoD) response to the GAO draft report, GAO-07-461, "DEFENSE INFRASTRUCTURE: Actions Needed to Guide DoD's Efforts to Identify, Prioritize, and Assess Its Critical Infrastructure," dated April 12, 2007 (GAO Code 350877). DoD concurs with comment to all six recommendations in the report.

Our point of contact for this action is Mr. William Bryan, OASD (HD&ASA), (703) 602-5730 ext. 143 or William.bryan@osd.mil.

Sincerely,

Peter F. Verga
Acting

Enclosure:
As stated

**GAO DRAFT REPORT - DATED APRIL 12, 2007**
**GAO CODE 350877/GAO-07-461**

**"DEFENSE INFRASTRUCTURE: Actions Needed to Guide DoD's Efforts to Identify, Prioritize, and Assess Its Critical Infrastructure"**

**DEPARTMENT OF DEFENSE COMMENTS TO THE RECOMMENDATIONS**

**RECOMMENDATION 1:** The GAO recommends that the Secretary of Defense direct the Office of the Assistant Secretary of Defense (Homeland Defense and Americas' Security Affairs) to develop and implement a comprehensive management plan that addresses guidance, coordination of stakeholders' efforts, and resources needed to implement the Defense Critical Infrastructure Program (DCIP). The plan should include the following actions:

- Establish timelines for finalizing the following draft DCIP guidance and policies:
  - DCIP Data Collection Essential Elements of Information
  - DCIP Interim Implementation Guidance
  - DCIP Integrated Risk Assessment Handbook
- Assist the defense sector lead agents in identifying, prioritizing, and including DCIP funding requirements through the regular budgeting process beginning in FY 2010.
- In coordination with the DoD Components, determine funding levels and sources needed to avoid reliance on supplemental appropriations and identify funding for DCIP remediation.

**DOD RESPONSE:** Concur with comment. Development of a DCIP Program Plan is underway and will be completed by September 2007. The DCIP Interim Implementation Guidance document was published on July 13, 2006. The DCIP Integrated Risk Assessment Handbook will not be published as a separate document; however, sections of the document will be published as appropriate. DCIP Data Collection Essential Elements of Information are under review by the community and disposition will be determined based on community comments. The DCIP Criticality Process Guidance Document (CPGD) was published on December 21, 2006. The DCIP Assessment Standards and Benchmarks was published on June 9, 2006. Other guidance documents will be published as appropriate.

**RECOMMENDATION 2:** The GAO recommends that the Secretary of Defense direct the Director of Administration and Management to issue a chartering directive to, among other things, define the relationship between the Directorates for Homeland Defense and Americas' Security Affairs and Special Operations and Low-Intensity Conflict & Interdependent Capabilities.

1

**DOD RESPONSE:** Concur. A chartering DoD directive has been drafted and is undergoing coordination with the ASD (HD&ASA). Following that it will be coordinated with the remainder of the Department beginning in late May; coordination should be completed by the end of June. Publication should be expected in July 2007.

**RECOMMENDATION 3:** The GAO recommends that the Secretary of Defense direct the Office of the Assistant Secretary of Defense (Homeland Defense and Americas' Security Affairs) to complete the identification and prioritization of critical infrastructure before increasing the number of infrastructure vulnerability assessments performed.

**DOD RESPONSE:** Concur with comment. While prioritization is dependent on the completion of the identification process, assessment is not. Vulnerability assessments are a valid tool for addressing risk and support risk management decisions at all levels. Delaying vulnerability assessments until all assets are identified is unnecessary and may delay the identification of vulnerabilities and remediation activities.

Assessments can be conducted incrementally while the identification process is underway. DoD components with existing infrastructure assessment programs and resources should be allowed to continue efforts in support of DoD's risk management approach. Additionally, an infrastructure vulnerability self-assessment program should also be allowed to progress. The identification and prioritization process is underway and should be complete by 2009.

**RECOMMENDATION 4:** The GAO recommends that the Secretary of Defense direct the Office of the Assistant Secretary of Defense (Homeland Defense and Americas' Security Affairs) to adopt the practice of combining the Defense Critical Infrastructure Vulnerability Assessment module with an existing assessment as the DoD-wide practice.

**DOD RESPONSE:** Concur with comment. DCIP currently combines its Defense Critical Infrastructure module with the Joint Staff Integrated Vulnerability Assessments and encourages other organizations performing assessments (e.g. Military Services, Agencies, etc.) to incorporate the Defense Critical Infrastructure Program (DCIP) module into their assessments. In addition, the issue of multiple DoD assessments is being addressed in the Joint Capabilities and Integration Development (JCID) process, lead by the Joint Staff (J34) that will recommend an appropriate analysis and assessment capability for the Department.

**RECOMMENDATION 5:** The GAO recommends that the Secretary of Defense direct the Office of the Assistant Secretary of Defense (Homeland Defense and Americas' Security Affairs) to issue guidance and criteria for performing infrastructure vulnerability self-assessments.

**DOD RESPONSE:** Concur. The Office of the Assistant Secretary of Defense (Homeland Defense and Americas' Security Affairs) has published the DCIP Assessment Standards and Benchmarks, version 1.0, on June 9, 2006 to provide guidance and criteria for performing infrastructure vulnerability assessments. These standards and benchmarks would apply to both onsite assessments as well as self assessments.

**RECOMMENDATION 6:** The GAO recommends that the Secretary of Defense direct the Office of the Assistant Secretary of Defense (Homeland Defense and Americas' Security Affairs) to identify and prioritize domestic non-DoD-owned critical infrastructure for the Department of Homeland Security to consider including among its assessments of the nation's critical infrastructure.

**DOD RESPONSE:** Concur. Defense Critical Infrastructure Program is working with the Department of Homeland Security on information sharing procedures and safeguards.

3

# Appendix III: GAO Contact and Staff Acknowledgments

## GAO Contact

Davi M. D'Agostino, (202) 512-5431, or dagostinod@gao.gov

## Acknowledgments

Mark A. Pross, Assistant Director; Burns D. Chamberlain; Alissa Czyz; Michael Gilmore; Cody Goebel; James Krustapentus; Kate Lenane; Thomas C. Murphy; Maria-Alaina Rambus; Terry Richardson; Jamie A. Roberts; Marc Schwartz; and Tim Wilson made key contributions to this report.

## GAO's Mission

The Government Accountability Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

## Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "Subscribe to Updates."

## Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

## To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

## Congressional Relations

Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, D.C. 20548

## Public Affairs

Paul Anderson, Managing Director, AndersonP1@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548